(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 17 362 A 1**

(51) Int. Cl.[7]: G 07 C 15/00

(21) Aktenzeichen: 101 17 362.8
(22) Anmeldetag: 6. 4. 2001
(43) Offenlegungstag: 17. 10. 2002

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Viering, Jentschura & Partner, 80538 München

(72) Erfinder:
Brederlow, Ralf, Dr., 81737 München, DE

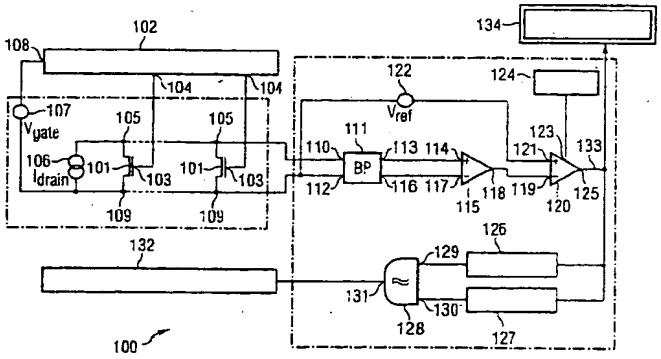
(56) Entgegenhaltungen:
US 62 47 033 B1
US 43 48 931 A
US 41 76 399 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Zufallszahlengenerator und Verfahren zum Erzeugen einer Zufallszahl

(57) Ein Zufallszahlengenerator weist eine Anzahl von Halbleiterbauelementen mit im Durchschnitt einer elektrisch aktiven Störstelle im für die Verarbeitung wichtigen Frequenzband in seiner Kristallstruktur auf. Mit einer Besetzungs-Erfassungseinheit wird ein geeigneter Transistor ausgewählt und dessen Besetzung oder eine Änderung der Besetzung in der elektrisch aktiven Störstelle des ausgewählten Transistors ermittelt. Mit einer Zufallszahlen-Umsetzungseinheit wird aus der ermittelten Besetzung oder der Änderung der Besetzung eine Zufallszahl gebildet.



DE 101 17 362 A 1

DE 101 17 362 A 1

Beschreibung

[0001] Die Erfindung betrifft einen Zufallszahlengenerator und ein Verfahren zum Erzeugen einer Zufallszahl.

[0002] Ein solcher Zufallszahlengenerator und ein solches Verfahren zum Erzeugen einer Zufallszahl sind aus [1] bekannt.

[0003] Bei dem in [1] beschriebenen Zufallszahlengenerator wird das thermische Rauschen und das 1/f-Rauschen eines elektronischen Bauelements als statistische Referenz zum Erzeugen einer Zufallszahl verwendet.

[0004] Weiterhin ist in [2] beschrieben, als statistische Referenz für das Erzeugen einer Zufallszahl die Korrelation zweier mit Phasenrauschen behafteter Oszillatoren zu verwenden.

[0005] Beide auf oben beschriebene Weise erzeugten Signale sind statistisch gaussverteilt und relativ klein.

[0006] Damit ergibt sich bei diesen bekannten Realisierungsmöglichkeiten für eine statistische Referenz zum Erzeugen einer Zufallszahl das Problem, die Gaussverteilung der kleinen Signale in eine Gleichverteilung der resultierenden Zufallsbits umzuwandeln, um eine möglichst verlässliche und geeignete Erzeugung von Zufallszahlen zu gewährleisten.

[0007] Hierzu müssen zur Umwandlung der Rauschgröße in eine Zufallszahl ein oder mehrere Oszillatoren verwendet werden.

[0008] Um weiterhin ein gaussverteiltes Signal in eine gleichverteilte Folge von Zufallszahlen umzuwandeln ist ein erheblicher zusätzlicher schaltungstechnischer oder systemtechnischer Aufwand erforderlich.

[0009] Weiterhin ist es bekannt, dass bei einem Halbleiterbauelement in dessen Kristallstruktur insbesondere bei einem Halbleiterbauelement, welches mit den mit modernen Prozesstechniken möglichen minimalen Bauelementgrößen hergestellt ist, sich wenige elektrisch aktive Störstellen befinden.

[0010] Insbesondere befinden sich nur sehr wenige elektrisch aktive Störstellen in einem kleinen CMOS-Feldeffekttransistor. Diese elektrisch aktiven Störstellen haben jedoch einen relativ großen Einfluss auf den durch den Transistor fließenden elektrischen Strom.

[0011] Jede elektrisch aktive Störstelle weist zwei unterschiedliche Störstellenzustände auf, die von der jeweiligen elektrisch aktiven Störstelle zu unterschiedlichen Zeitpunkten jeweils angenommen werden können.

[0012] Die Veränderung der Störstellenzustände wird im Weiteren auch als Änderung der Belegung oder Besetzung der Störstelle mit Ladungsträgern bezeichnet.

[0013] Die Besetzung der Störstellen bzw. die Veränderung der Besetzung der Störstellen führt zu einem zeitlichen Signalverlauf in dem Halbleiterbauelement, anders ausgedrückt zu einem zeitlichen Rauschverhalten des Halbleiterbauelements. Das erzeugte Signal wird auch als Random Telegraph Signal (RTS) bezeichnet.

[0014] Somit liegt der Erfindung das Problem zu Grunde, einen Zufallszahlengenerator sowie ein Verfahren zum Erzeugen einer Zufallszahl anzugeben, bei dem die Aufbereitung von Signalen zu einer gleichverteilten zufälligen Bitfolge vereinfacht wird oder bei dem eine Linearisierung der Signale zu der gleichverteilten zufälligen Bitfolge gar nicht erforderlich ist.

[0015] Das Problem wird durch den Zufallszahlengenerator sowie durch das Verfahren zum Erzeugen einer Zufallszahl mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

[0016] Ein Zufallszahlengenerator weist ein Halbleiterbauelement auf mit mindestens einer elektrisch aktiven Störstelle in dessen Kristallstruktur. Mit dem Halbleiterbauelement ist eine Besetzungs-Erfassungseinheit gekoppelt. Die Besetzungs-Erfassungseinheit ist derart eingerichtet, dass eine Besetzung oder eine Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt werden kann. Ferner ist eine Zufallszahlen-Umsetzungseinheit vorgesehen, die mit der Besetzungs-Erfassungseinheit gekoppelt ist. Die Zufallszahlen-Umsetzungseinheit ist derart eingerichtet, dass aus der ermittelten Besetzung oder der ermittelten Änderung der Besetzung in der elektrisch aktiven Störstelle eine Zufallszahl gebildet wird.

[0017] Unter einer elektrisch aktiven Störstelle ist eine Störstelle in einem Kristallgitter eines Halbleiterbauelements zu verstehen, die aufgrund ihrer Besetzung mit einem Ladungsträger zwei unterschiedliche Störstellenzustände aufweist, was zu einem zeitlichen Rauschverhalten führt, wie es im Weiteren näher erläutert wird. Das zeitliche Rauschverhalten des Halbleiterbauelements ist statistisch poissonverteilt.

[0018] Anders ausgedrückt bedeutet dies, dass unabhängig vom Startzeitpunkt der Betrachtung bzw. des nächsten Übergangs von einem Besetzungszustand in einen anderen Besetzungszustand in der Störstelle die Wahrscheinlichkeit für einen solchen Wechsel proportional zum negativen Exponenten der Zeitdifferenz zum Beginn des Betrachtungszeitraums ist. Diese Eigenschaft entspricht somit der statistischen Abhängigkeit der Poissonverteilung.

[0019] n elektrisch aktive Störstellen in einem Kristallgitter eines Halbleiterbauelements weisen somit 2^n unterschiedliche Störstellenzustände in dem Halbleiterbauelement auf.

[0020] Bei einem Verfahren zum Erzeugen einer Zufallszahl wird bei einem Halbleiterbauelement, welches mindestens eine elektrisch aktive Störstelle in dessen Kristallstruktur aufweist, eine Besetzung oder eine Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt, anschaulich die Änderung des Rauschstromes und/oder der Rauschspannung Halbleiterbauelements aufgrund der Besetzung oder der Änderung der Besetzung in der elektrisch aktiven Störstelle. Aus der ermittelten Besetzung oder der ermittelten Änderung der Besetzung in der elektrisch aktiven Störstelle wird eine Zufallszahl gebildet.

[0021] Durch die Erfindung wird ein Zufallszahlengenerator und ein Verfahren zum Erzeugen einer Zufallszahl angegeben, welches mit geringerem schaltungstechnischen oder systemtechnischer Aufwand in ein gleichverteiltes Signal überführbar ist.

[0022] Der erfindungsgemäße Zufallszahlengenerator und das erfindungsgemäße Verfahren sind ferner sehr einfach und in ihr sehr kleiner Dimension als elektronische Schaltung, vorzugsweise als integrierte Schaltung, realisierbar.

[0023] Weiterhin ist bei dem erfindungsgemäßen Zufallszahlengenerator eine wichtige Voraussetzung für einen verlässlichen Zufallszahlengenerator erfüllt, da die Besetzung oder die Änderung der Besetzung einer Störstelle bei konstant gehaltener äußerer elektrischen Spannung an dem Halbleiterbauelement in sehr guter Näherung unabhängig von den zu der elektrisch aktiven Störstelle benachbarter Nachbarstörstellen ist und somit die Wahrscheinlichkeit für einen Übergang von einem Besetzungszustand in einen anderen Besetzungszustand nur von der Vorgeschichte, d. h. von den zeitlich vorangegangenen Besetzungszuständen der elektrisch aktiven Störstelle selbst und dem aktuellen Besetzungszustand der betrachteten elektrisch aktiven Störstelle abhängt.

[0024] Anschaulich kann die Erfindung teilweise darin gesehen werden, dass das Rauschverhalten einer elektrisch aktiven Störstelle in einem Halbleiterbauelement, vorzugs-

weise in einem CMOS-Feldeffekttransistor, verwendet wird, um als statistische Referenz für das Erzeugen einer Zufallszahl zu dienen.

[0025] Es ist in diesem Zusammenhang darauf hinzuweisen, dass das erfindungsgemäße Ausnutzen des erzeugten RTS-Signals als statistische Referenz zum Erzeugen einer Zufallszahl nicht beschränkt ist auf einen Feldeffekttransistor. Die Erfindung kann bei jedem Halbleiterbauelement eingesetzt werden, das ein solches RTS-Signal erzeugen kann.

[0026] Da im Gegensatz zu bisherigen Auslese verfahren kein Referenzsignal durch ein weiteres durch Phasenrauschen mit statistischen Eigenschaften behaftetes Signal abgetastet wird und das statistische Signal nicht gaussverteilt ist, wie dies beispielsweise in [1] der Fall ist, wird erfindungsgemäß eine Extremwertkorrektur nicht benötigt.

[0027] Es ist in diesem Zusammenhang anzumerken, dass für den Fall, dass als Auswertungskriterium des RTS-Signals für die statistische Referenz die Änderung des Besetzungszustandes in der Störstelle verwendet wird kein Problem einer sonst erforderlichen Linearisierung auftritt, d. h. es ist in diesem Fall keine Linearisierung erforderlich, da die Änderung des Besetzungszustandes ohnehin gleichverteilt ist. Dies gilt zumindest für den Fall, dass das Zeitfenster, d. h. der Zeitraum, in welchem jeweils das RTS-Signal betrachtet wird, ausreichend groß ist und eine geeignete Störstelle bei einer geeigneten Gate-Source-Spannung gefunden ist.

[0028] Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

[0029] Das Halbleiterbauelement kann ein in MOS-Technologie hergestelltes Halbleiterelement sein.

[0030] Gemäß einer Weiterbildung der Erfindung ist das Halbleiterbauelement ein in CMOS-Technologie hergestelltes Halbleiterbauelement.

[0031] Gemäß einer anderen Ausgestaltung der Erfindung ist das Halbleiterbauelement ein Feldeffekttransistor, vorzugsweise ein CMOS-Feldeffekttransistor.

[0032] Bei einem CMOS-Feldeffekttransistor ist es bei Kenntnis der Störstellendichte möglich, den jeweiligen CMOS-Feldeffekttransistor so zu dimensionieren, dass statistisch betrachtet im Durchschnitt zumindest in einem vorgegebenen Frequenzbereich genau eine elektrisch aktive Störstelle in dem Kristallgitter des CMOS-Feldeffekttransistors, vorzugsweise an der Silizium/Siliziumdioxid-Grenzfläche des CMOS-Feldeffekttransistors, vorhanden ist. Dies bedeutet, dass in diesem Fall durchschnittlich genau eine Störstelle rauschaktiv ist. Die Störstellendichte N_t kann gemäß einer üblichen Vorgehensweise ermittelt werden, beispielsweise durch Messen des Rauschens in dem Halbleiterbauelement oder mittels des sogenannten "Charge-Pumping"-Verfahrens.

[0033] Beispielsweise ergibt sich bei einer Störstellendichte N_t von

$$N_t \left[\frac{\text{Störstellen}}{\text{cm}^2} \right] \approx 10^{10}$$

unter Verwendung der Beziehung

$N_t \cdot A = 1$,

in anderen Worten, unter der Voraussetzung, dass pro Feldeffekttransistor mit der Fläche A nur genau eine Störstelle im Durchschnitt vorhanden sein soll für die Fläche A des Feldeffekttransistors:

$$A = \frac{1}{N_t} = 10^{-2} \mu\text{m}^2 .$$

[0034] Diese Voraussetzung und diese Strukturgrößen sind in einem heutzutage üblichen CMOS-Prozess zur Herstellung eines CMOS-Feldeffekttransistors gegeben.

[0035] In anderen Worten ausgedrückt, der Feldeffekttransistor ist gemäß einer Ausgestaltung der Erfindung derart dimensioniert, dass er im statistischen Durchschnitt genau eine elektrisch aktive Störstelle in einem vorgegebenen gewünschten, üblicherweise im später verarbeiteten Frequenzbereich (Frequenzband) aufweist.

[0036] Gemäß einer Ausgestaltung der Erfindung ist es vorgesehen, dass die Zufallszahlen-Umsetzungs-Einheit derart eingerichtet ist, dass jeweils in einem Abstand einer vorgegebenen, vorzugsweise konstanten, Zeitdauer die Besetzung oder die Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt werden kann.

[0037] Dies entspricht anschaulich der Verwendung eines Zeitfensters, mit dem jeweils das Rauschverhalten "abgefragt", d. h. ermittelt wird.

[0038] Es wird jeweils ermittelt, ob aufgrund des ermittelten Signals in dem jeweils betrachteten Zeitfenster dem Signalverlauf in dem Zeitfensters ein erster logischer Wert "0" oder ein zweiter logischer Wert "1" zugeordnet wird.

[0039] Die vorgegebene Zeitdauer, d. h. die Größe des Zeitfensters, sollte erheblich länger sein, d. h. einen Faktor von mindestens zwei aufweisen verglichen mit der durchschnittlichen Zeitdauer, in der ein Wechsel von einem Besetzungszustand in einen anderen Besetzungszustand erfolgt, damit die in jeweils einen Bit-Wert übersetzten Umladungsereignisse statistisch voneinander unabhängig sind, und somit dass die Bits, welche die jeweilige Zufallszahl repräsentieren, statistisch voneinander unabhängig sind.

[0040] Um die vorgegebene Zeitdauer ermitteln zu können, sollte vorteilhafterweise das Zeitverhalten des Störstellenzustands bekannt sein oder es sollten, wie im Weiteren noch näher erläutert wird, eine Mehrzahl verschiedener Halbleiterbauelemente, vorzugsweise eine Mehrzahl verschiedener CMOS-Feldeffekttransistoren zur Verfügung stehen, von dem zumindest einer das zuvor gewählte Zeitverhalten, an dem die vorgegebene Zeitdauer ausgerichtet ist, aufweist, so dass in den jeweiligen Zeitfenstern voneinander statistisch unabhängige Signalverläufe ermittelt werden.

[0041] Die Zufallszahlen-Umsetzungs-Einheit kann derart eingerichtet sein, dass die vorgegebene Zeitdauer um ein Mehrfaches länger ist als eine durchschnittliche Zeit einer Änderung der Besetzung in der elektrisch aktiven Störstelle.

[0042] Gemäß einer weiteren Ausgestaltung der Erfindung ist eine Mehrzahl, vorzugsweise eine Vielzahl von Halbleiterbauelement vorgesehen mit jeweils mindestens einer elektrisch aktiven Störstelle in der Kristallstruktur des jeweiligen Halbleiterbauelements. Die Besetzungs-Erfassungseinheit ist in diesem Fall mit allen Halbleiterbauelementen gekoppelt. Ferner ist eine Halbleiterbauelement-Auswahleinheit zum Auswählen eines Halbleiterbauelements der Mehrzahl von Halbleiterbauelementen, bei welchem Halbleiterbauelement die Besetzung oder die Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt werden soll.

[0043] Damit kann aus statistischen Gründen bei einer ausreichenden Anzahl vorhandener Halbleiterbauelemente auf eine Justierung (P("Störstelle unbesetzt") = P("Störstelle besetzt") = 0,5) verzichtet werden, da ohnehin eine ausreichende Anzahl von Halbleiterbauelementen mit den gewünschten Eigenschaften verfügbar ist, welche mittels der

Halbleiterbauelement-Auswahleinheit ausgewählt werden können.

[0044] Es ist in diesem Zusammenhang anzumerken, dass bei dem Zufallszahlengenerator gemäß dieser Ausgestaltung der Erfindung anschaulich ein zweifacher Zufallsprozess auftritt. Es ist nämlich einerseits schon zufällig, bei einem Halbleiterbauelement, vorzugsweise bei einem Transistor, überhaupt ein RTS-Rauschsignal erzeugt wird. Tritt bei einem der Vielzahl der Halbleiterbauelemente ein RTS-Rauschsignal auf, so ist dessen Verlauf ebenfalls zufällig. Die Anzahl der Halbleiterbauelemente in dem Zufallszahlengenerator sollte so gewählt sein, dass gemäß den bereits erwähnten statistischen Regeln ein oder mehrere Halbleiterbauelemente in dem Zufallszahlengenerator enthalten sind, in denen ein gewünschtes RTS-Rauschsignal erzeugt wird.

[0045] Gemäß einer weiteren Ausgestaltung der Erfindung ist eine Gate-Spannungs-Justierienrichtung vorgesehen, mittels der die an dem Feldeffekttransistor anliegende Gate-Spannung eingestellt werden kann. Auf diese Weise wird es sehr einfach möglich, die Zeitkonstante für die mittlere Übergangszeit eines Besetzungszustandes in der Störstelle zu justieren.

[0046] Alternativ zum oder in Kombination mit dem Ermitteln eines Halbleiterbauelements mit einer geeigneten Störstelle aus einer Vielzahl von Halbleiterbauelementen kann auch eine einfache Justierung der entsprechenden Wahrscheinlichkeit vorgenommen werden.

[0047] Ist die Häufigkeit des Auftretens des Zustandes der Störstelle "Störstelle besetzt" ("1"-Zustand) nicht gleich groß wie die Häufigkeit des Auftretens des Zustandes "Störstelle unbesetzt" ("0"-Zustand), so kann mittels des folgenden Verfahrens wieder eine gleiche Verteilung von "0"-Zustand und "1"-Zustand erreicht werden.

[0048] Gemäß diesem Verfahren wird anstatt des "0"-Zustandes und des "1"-Zustandes der Störstelle das Auftreten des Übergangs der Störstelle von dem unbesetzten Zustand in den besetzten Zustand (von dem "0"-Zustand in den "1"-Zustand) oder umgekehrt von dem besetzten Zustand in den unbesetzen Zustand (von dem "1"-Zustand in den "0"-Zustand) detektiert.

[0049] In diesem Fall wird der neue "1"-Zustand durch das Detektieren mindestens eines Übergangs, der neue "0"-Zustand durch das Fehlen eines solchen Ereignisses definiert.

[0050] Durch die Wahl eines geeigneten Zeitfensters für die Entscheidung ist wieder eine gleich große Wahrscheinlichkeit für beide neuen Zustände möglich.

[0051] In diesem Zusammenhang sollte noch erwähnt werden, dass sinnvollerweise die Übergänge von dem wahrscheinlicheren Zustand in den unwahrscheinlicheren Zustand detektiert werden sollten.

[0052] Weiterhin kann eine Spannungsquelle vorgesehen sein, die mit der Halbleiterbauelement-Auswahleinheit derart gekoppelt ist, dass die Halbleiterbauelement-Auswahleinheit die von der Spannungsquelle bereitgestellte elektrische Spannung an dem Gate-Anschluss des ausgewählten Feldeffekttransistors der Mehrzahl der Feldeffekttransistoren anlegt. Die Drain-Anschlüsse aller Feldeffekttransistoren sind gemäß dieser Ausgestaltung der Erfindung mit der Besetzungs-Erfassungseinheit gekoppelt.

[0053] Die Besetzungs-Erfassungseinheit kann einen Bandpass-Filter aufweisen, dessen erster Eingang mit den Drain-Anschlüssen der Feldeffekttransistoren gekoppelt ist und dessen zweiter Eingang mit den Source-Anschlüssen der Feldeffekttransistoren gekoppelt ist.

[0054] Mit dem Bandpass-Filter wird der Störeffekt, der von eventuell vorhandenen weiteren elektrisch aktiven Störstellen erzeugt wird, reduziert.

[0055] Es ist in diesem Zusammenhang anzumerken, dass dieser Störeffekt auch durch eine ausreichende Anzahl von bereitgestellten Halbleiterbauelementen, vorzugsweise CMOS-Feldeffekttransistoren, abgefangen werden kann.

[0056] Ferner kann die Besetzungs-Erfassungseinheit einen Differenzverstärker aufweisen, der zwischen das Bandpass-Filter und die Zufallszahlen-Umsetzungseinheit geschaltet ist und der das RTS-Signal auf einen vorgegebenen, vorzugsweise logischen, Pegel verstärkt.

[0057] Die Zufallszahlen-Umsetzungseinheit kann als Komparator ausgestaltet sein.

[0058] Ausführungsbeispiele der Erfindung sind in den Figuren dargestellt und werden im Weiteren näher erläutert.

[0059] Es zeigen

[0060] **Fig.** 1 eine Prinzipskizze eines Zufallszahlengenerators gemäß einem Ausführungsbeispiel der Erfindung;

[0061] **Fig.** 2a und 2b einen Signalverlauf eines RTS-Signals in einem Halbleiterbauelement im zeitlichen Verlauf (**Fig.** 2a) und im Frequenzraum (**Fig.** 2b);

[0062] **Fig.** 3 ein Rauschspektrum von minimalen CMOS-Feldeffekttransistoren, hergestellt in einem CMOS-Prozess mit einer minimalen Strukturgröße von 0,25 µm;

[0063] **Fig.** 4 den Signalverlauf des RTS-Signals aus **Fig.** 2a mit symbolisierten Zeitfenstern;

[0064] **Fig.** 5 eine schaltungstechnische Realisierung eines Zufallszahlengenerators gemäß einem Ausführungsbeispiel der Erfindung;

[0065] **Fig.** 6 eine Skizze eines Zufallszahlengenerators gemäß einem weiteren Ausführungsbeispiel der Erfindung.

[0066] **Fig.** 1 zeigt einen Zufallszahlengenerator **100** gemäß einem ersten Ausführungsbeispiel der Erfindung.

[0067] Der Zufallszahlengenerator **100** weist eine Vielzahl von CMOS-Feldeffekttransistoren **101** als eine Vielzahl von Halbleiterbauelementen auf, sowie eine Feldeffekttransistoren-Auswahleinheit **102** zum Auswählen zumindest eines CMOS-Feldeffekttransistors **101**.

[0068] Die CMOS-Feldeffekttransistoren **101** weisen eine Gatelänge von 0,13 µm und eine Gatelänge von ebenfalls 0,13 µm auf. Jeder CMOS-Feldeffekttransistor **101** weist mindestens eine elektrisch aktive Störstelle auf, mittels der ein in **Fig.** 2a symbolisch als Rauschsignal **201** in der zeitlichen Darstellung dargestelltes Rauschverhalten erzeugt wird.

[0069] Das Rauschsignal **201** stellt anschaulich ein Generations-/Rekombinationsrauschen als Zufallssignal im Zeitraum entlang der Zeitachse t dar.

[0070] **Fig.** 2b zeigt das Rauschsignal **201** in logarithmierter Darstellung im Frequenzspektrum als Frequenzsignal **202**.

[0071] **Fig.** 3 zeigt beispielhaft einige Rauschspektren **301** von CMOS-Feldeffekttransistoren, die mit einer CMOS-Technologie mit einer minimalen Strukturgröße von 0,25 µm hergestellt worden sind.

[0072] Der Gate-Anschluss **103** jedes CMOS-Feldeffekttransistors **101** ist jeweils an einen Ausgang **104** der Feldeffekttransistoren-Auswahleinheit **102**, d. h. anschaulich einem Dekoder, angeschlossen.

[0073] Ferner ist der Drain-Anschluss **105** eines jeden CMOS-Feldeffekttransistors **101** mit einer Stromquelle **106** gekoppelt. Über eine Spannungsquelle **107**, die eine Gate-Spannung V_{Gate} bereitstellt, ist ein Eingang **108** der Feldeffekttransistoren-Auswahleinheit **102** mit dem Source-Anschluss **109** eines jeden CMOS-Feldeffekttransistors **101** gekoppelt.

[0074] Mittels der Feldeffekttransistoren-Auswahleinheit **102** wird ein CMOS-Feldeffekttransistor **101** ausgewählt, in dem an den Gate-Anschluss **103** des ausgewählten CMOS-Feldeffekttransistor **101** die Gate-Spannung V_{Gate} angelegt

wird.

[0075] Die Drain-Anschlüsse **105** aller CMOS-Feldeffekttransistoren **103** sind mit einem ersten Eingang **110** eines Bandpass-Filters **111** gekoppelt. Die Source-Anschlüsse **109** aller CMOS-Feldeffekttransistoren **103** sind mit einem zweiten Eingang **112** des Bandpass-Filters **111** gekoppelt.

[0076] Ein erster Ausgang **113** des Bandpass-Filters **111** ist mit einem nicht-invertierenden Eingang **114** eines Differenzverstärkers **115** gekoppelt. Ferner ist ein zweiter Ausgang **116** des Bandpass-Filters **111** mit dem invertierenden Eingang **117** des Differenzverstärkers **115** gekoppelt.

[0077] Der Ausgang **118** des Differenzverstärkers **115** ist mit: dem invertierenden Eingang **119** eines getakteten Komparators **120** gekoppelt, dessen nicht-invertierender Eingang **121** über eine Referenz-Spannungsquelle **122** (die eine Referenzspannung V_{ref} bereitstellt) mit den Source-Anschlüssen **109** aller CMOS-Feldeffekttransistoren **101** gekoppelt ist.

[0078] Der getaktete Komparator **120** weist ferner einen Takteingang **123** auf und wird über diesen mittels eines Taktsignals **124** getaktet.

[0079] Anschaulich wird somit mittels des Dekoders, d. h. mittels der Feldeffekttransistoren-Auswahleinheit **102** die von der Gate-Spannungsquelle **107** bereitgestellte Gate-Source-Spannung V_{Gate} an den ausgewählten CMOS-Feldeffekttransistor **101** durchgeschaltet, wobei alle anderen, nicht ausgewählten CMOS-Feldeffekttransistoren **101** mit einer Gate-Source-Spannung $V_{Gate} = 0$ angesteuert werden.

[0080] Das jeweilige Rauschsignal, das über den Source-Anschluss **109** und den Drain-Anschluss **105** des ausgewählten CMOS-Feldeffekttransistors **101** fließt, wird anschaulich über den Bandpass-Filter **111** und den Differenzverstärker **115** auf den getakteten Komparator **120** geleitet, der das Rauschsignal mit einem Referenzsignal, d. h. der Referenzspannung V_{ref} vergleicht und daraus einen dem von dem CMOS-Feldeffekttransistor **101** erzeugten Rauschsignal entsprechenden ersten logischen Wert "0" oder zweiten logischen Wert "1" als ein Zufallsignal **133** an dem Ausgang **125** des Komparators **120** erzeugt.

[0081] Der Ausgang **125** des Komparators **120** ist ferner mit einem ersten Zähler **126** gekoppelt sowie mit einem zweiten Zähler **127**. Mittels des ersten Zählers **126** wird die Auftrittshäufigkeit eines Signals mit dem ersten logischen Wert "0" gezählt und mittels des zweiten Zählers **127** wird die Auftrittshäufigkeit eines Signals mit dem zweiten logischen Wert "1" an dem Ausgang **125** des Komparators **120** gezählt.

[0082] Die beiden Zähler **126** und **127** sind über ein UND-Gatter **128** mit einem Speicher **132** gekoppelt. Der erste Zähler **126** ist mit einem ersten Eingang **129** des UND-Gatters **128** gekoppelt und der zweite Zähler **127** ist mit einem zweiten Eingang **130** des UND-Gatters **128** gekoppelt. Der Ausgang **131** des UND-Gatters **128** ist mit dem Speicher **132** gekoppelt.

[0083] Es ist in diesem Zusammenhang anzumerken, dass sowohl die Gate-Spannung V_{Gate} als auch die Referenzspannung V_{ref} optional variiert werden können oder über eine zusätzliche Rückkopplungsschleife mittels einer nicht dargestellten Justiereinrichtung nachjustiert, d. h. angepasst werden können.

[0084] Für diesen Fall wird der Speicher **132** verwendet, um die geeigneten Zustände zu jeder Gate-Spannung V_{Gate} zu speichern und diese entsprechend den Umgebungsbedingungen zu verändern.

[0085] Da das statistische Verhalten der elektrisch aktiven Störstellen und deren örtliche Anordnung entlang der Oberfläche des jeweiligen CMOS-Feldeffekttransistors **101** bekannt ist, kann eine für eine hohe Ausbeutung von integrierten Schaltungen notwendige Zahl von CMOS-Feldeffekttransistoren **101** pro elektrische Schaltung auf einfache Weise berechnet werden.

[0086] Mittels der Feldeffekttransistoren-Auswahleinheit **102** wird somit ein geeigneter CMOS-Feldeffekttransistor **101** auf der Basis eines zuvor durchgeführten Kalibrierungsverfahrens ausgewählt, wobei im Rahmen des Kalibrierungsverfahrens das Zeitverhalten, d. h. die zeitliche Veränderung der Störstellenzustände des jeweiligen CMOS-Feldeffekttransistors **101** ermittelt wird.

[0087] Als Ergebnis des Kalibrierungsverfahrens erhält man den für den Zufallszahlengenerator **100** am besten geeigneten CMOS-Feldeffekttransistor **101**, das heißt denjenigen CMOS-Feldeffekttransistor **101**, bei dem die Wahrscheinlichkeit für einen ersten Besetzungszustand P(1) ungefähr gleich ist der Wahrscheinlichkeit für das Vorliegen des zweiten Besetzungszustandes P(0).

[0088] Das Kalibrierungsverfahren muss in den meisten Fällen nur ein Mal durchgeführt werden, da die Übergangswahrscheinlichkeit der Störstelle in dem jeweiligen CMOS-Feldeffekttransistor **101** bei geeignetem Aufbau der Spannungsquelle **107** für den ausgewählten CMOS-Feldeffekttransistor **101** nur in geringem Maße von den äußeren Randbedingungen, beispielsweise einer Versorgungsspannungs-Schwankung oder einer Temperaturschwankung, abhängen.

[0089] Da die Zeitkonstante für die mittlere Übergangszeit der Störstelle von einem ersten Besetzungszustand in einen zweiten Besetzungszustand und umgekehrt eine Funktion der jeweils angelegten Gate-Spannung ist, kann die Zeitkonstante in einem gewissen Rahmen justiert, d. h. eingestellt werden durch Veränderung der jeweils angelegten Gate-Spannung.

[0090] Die Einstellbarkeit der Zeitkonstante kann genutzt werden, um die gewünschte Gleichverteilung der beiden Wahrscheinlichkeiten $P(0) = P(1) = 0,5$ zu erzielen.

[0091] Alternativ kann zum Erreichen der Gleichverteilung der beiden Wahrscheinlichkeiten $P(0) = P(1) = 0,5$ die Änderung des Besetzungszustandes einer Störstelle entweder von dem Besetzungszustand "besetzt" zu dem Besetzungszustand "unbesetzt" oder von dem Besetzungszustand "unbesetzt" zu dem Besetzungszustand "besetzt" erfasst werden.

[0092] Steht eine ausreichende Zahl von CMOS-Feldeffekttransistoren **101** als mögliche Quelle für den Zufallszahlengenerator **100** zur Verfügung, so ist eine Justierung üblicherweise nicht erforderlich, da man die Zahl der zur Verfügung stehenden CMOS-Feldeffekttransistoren **101** so einstellen kann, dass mit einer Wahrscheinlichkeit von fast 100 Prozent ein CMOS-Feldeffekttransistor **101** in der Vielzahl von CMOS-Feldeffekttransistoren **101** enthalten ist, der die gewünschten Bedingungen der Gleichverteilung des erzeugten Rauschsignals, d. h. $P(0) = P(1) = 0,5$, in ausreichender Genauigkeit erfüllt.

[0093] Da es sich bei dem CMOS-Feldeffekttransistoren **101** ohnehin um sehr kleine Feldeffekttransistoren handelt, verbrauchen die CMOS-Feldeffekttransistoren **101**, die der gewünschten Bedingungen nicht genügen, kaum Chipfläche.

[0094] Der Komparator **120** wird derart getaktet, dass in einem vorgegebenen Zeitabstand, der anschaulich jeweils ein Zeitfenster **401** bildet (vgl. **Fig. 4**), jeweils einen Ausgangssignalwert **124** an dem Ausgang **125** des Komparators **120** zu jeweils einem Ermittlungszeitpunkt **402** bereitgestellt wird. Der Wert des Ausgangssignals **124** zu jeweils einem Zeitpunkt eines Zeitfensters **401** bildet ein Bit der zu bildenden Zufallszahl **134**. In **Fig. 4** ist ein 6-Bit Zufallswort **403** als Zufallszahl **134** beispielhaft dargestellt.

[0095] Ein erheblicher Vorteil des Zufallszahlengenera-

tors **100** ist darin zu sehen, dass er im Gegensatz zu den Zufallszahlengeneratoren gemäß dem Stand der Technik

- kaum eine digitale Justierung benötigt und diese ohnehin nur im Rahmen der Initialisierung,
- keine komplizierten, möglichst hochauflösenden A/D-Wandler, und
- dass er einfach unabhängig von jeglichen (nicht-differentiellen) Referenzgrößen ausführbar ist.

[0096] Als Konsequenz daraus ist das erfindungsgemäße Verfahren zum Erzeugen einer Zufallszahl auch unempfindlich hinsichtlich eines Überkoppelns aus anderen Teilen einer größeren Schaltung, in der der Zufallszahlengenerator **100** integriert ist, sowie hinsichtlich nicht-statischer Einflüsse, die sich aus diesen Referenzgrößen ergeben.

[0097] **Fig.** 5 zeigt eine schaltungstechnische Realisierung des Zufallszahlengenerators **500**.

[0098] Der Zufallszahlengenerator **500** weist eine Mehrzahl von CMOS-Feldeffekttransistoren **501**, im Weiteren auch als Minimaltransistoren **501** bezeichnet, auf, welche im statistischen Durchschnitt jeweils eine elektrisch aktive Störstelle in ihrem Kristallgitter aufweisen. Die Störstelle ist jeweils derart eingerichtet, dass in dem Halbleiterbauelement ein RTS-Signal erzeugt wird, welches über den Kanalbereich des CMOS-Feldeffekttransistors **501** von dem jeweiligen Source-Anschluss **502** zu dem Drain-Anschluss **503** geleitet wird, wenn an dem Gate-Anschluss **504** eine ausreichend große Gate-Spannung $V_{Gate} \neq 0$ anliegt.

[0099] Der Gate-Anschluss **504** eines jeden CMOS-Feldeffekttransistors **501** ist mit jeweils einem Ausgang **505** des Dekoders **506** gekoppelt. Der Eingang **507** des Dekoders **506** ist mit einer Gate-Spannungsquelle **508** gekoppelt und darüber mit dem Massepotential **509**.

[0100] Zwischen die Gate-Spannungsquelle **508** und dem Eingang **507** des Dekoders **506** ist ein erster Anschluss **511** einer Offset-Spannungsquelle **510** geschaltet, deren zweiter Anschluss **512** mit dem Gate-Anschluss **513** eines ersten weiteren CMOS-Feldeffekttransistors **514** gekoppelt ist, dessen Source-Anschluss **515** mit den Source-Anschlüssen **502** der CMOS-Feldeffekttransistoren **501** gekoppelt ist.

[0101] Anstatt des ersten weiteren CMOS-Feldeffekttransistors **514** können alternativ eine Mehrzahl von Minimaltransistoren vorgesehen sein. Auf diese Weise wird die Symmetrie der Differenzstufe erhöht und damit ihre Unempfindlichkeit gegenüber äußeren Störungen. Das erfindungsgemäße Verfahren zum Erzeugen einer Zufallszahl wird davon jedoch nur mittelbar beeinflusst, da immer ein Paar von Minimaltransistoren an die Differenzstufe angeschlossen werden kann, von denen nur einer ein ausgeprägtes RTS-Signal aufweist.

[0102] Die Offset-Spannungsquelle **510** stellt eine Offset-Spannung V_{offset} bereit. Die Offset-Spannung dient zur Justierung von Halbleiterbauelementen-Mismatch.

[0103] Die Source-Anschlüsse **502** der CMOS-Feldeffekttransistoren **501** sowie der Source-Anschluss **515** des ersten weiteren CMOS-Feldeffekttransistors **514** sind mit dem Drain-Anschluss **516** eines zweiten weiteren CMOS-Feldeffekttransistors **517** gekoppelt, dessen Source-Anschluss **518** mit dem Massepotential **509** gekoppelt ist.

[0104] An den Gate-Anschluss **519** des zweiten weiteren CMOS-Feldeffekttransistor **517** sowie an die Gate-Anschlüsse **520** und **521** eines dritten weiteren CMOS-Feldeffekttransistors **522** und eines vierten weiteren CMOS-Feldeffekttransistors **523** ist eine Bias-Spannungsquelle **524** angeschlossen, die eine Bias-Spannung V_{Bias} bereitstellt.

[0105] Die Source-Anschlüsse **525** und **526** des dritten weiteren CMOS-Feldeffekttransistors **522** und des vierten weiteren CMOS-Feldeffekttransistors **523** sind ebenfalls mit dem Massepotential **509** gekoppelt.

[0106] Die Source-Anschlüsse **503** der CMOS-Feldeffekttransistoren **501** sind über einen ersten elektrischen Widerstand **527** mit dem Betriebspotential V_{DD} **528** gekoppelt.

[0107] Ferner sind die Source-Anschlüsse **503** der CMOS-Feldeffekttransistoren **501** mit dem Gate-Anschluss **59** eines fünften weiteren CMOS-Feldeffekttransistors **530** gekoppelt.

[0108] Der Drain-Anschluss **531** des ersten weiteren CMOS-Feldeffekttransistor **514** ist über einen zweiten elektrischen Widerstand **532** ebenfalls mit dem Betriebspotential V_{DD} **528** gekoppelt.

[0109] Ferner ist der Drain-Anschluss **531** des ersten weiteren CMOS-Feldeffekttransistors **514** mit dem Gate-Anschluss **533** eines sechsten weiteren CMOS-Feldeffekttransistors **534** gekoppelt, dessen Drain-Anschluss **535** ebenfalls mit dem Betriebspotential V_{DD} **528** gekoppelt ist.

[0110] Der Drain-Anschluss **536** des dritten weiteren CMOS-Feldeffekttransistors **522** ist mit dem Source-Anschluss **537** des sechsten weiteren CMOS-Feldeffekttransistors **534** und mit dem invertierenden Eingang **538** eines getakteten Komparators **539**, der mittels eines Zeitfenster-Steuerungssignals **540** über einen Takteingang **541** getaktet wird, gekoppelt.

[0111] Der Drain-Anschluss **542** des vierten weiteren CMOS-Feldeffekttransistor **523** ist mit dem Source-Anschluss **543** des fünften weiteren CMOS-Feldeffekttransistors **530**, dessen Drain-Anschluss **544** ebenfalls mit dem Betriebspotential V_{DD} **528** gekoppelt ist, und mit dem nicht-invertierenden Eingang **545** des getakteten Komparators **539** gekoppelt.

[0112] An dem Ausgang **546** des Komparators **539** liegt zu jeweils einem Zeitpunkt eines Zeitfensters ein Bit-Wert als Ausgangssignal-Wert an. Über die gesamte betrachtete Zeitdauer wird somit eine Folge von Bits als Zufallszahl **547** aus den jeweiligen Ausgangssignal-Werten erzeugt.

[0113] Der Ausgang **546** des Komparators **539** ist ferner mit einem ersten Zähler **548** zum Zählen der auftretenden Ausgangssignal-Werte mit einem ersten logischen Wert "0" und mit einem zweiten Zähler **549** zum Ermitteln der Auftrittshäufigkeit eines Ausgangs-Signalwerts mit einem zweiten logischen Wert "1" gekoppelt.

[0114] Die beiden Zähler **548** und **549** sind mit jeweils einem Eingang **550**, **551** eines logischen UND-Gatters **552** gekoppelt, dessen Ausgang **553** mit einem Speicher **554** gekoppelt ist.

[0115] In diesem Zusammenhang ist anzumerken, dass die schaltungstechnische Realisierung des Zufallszahlengenerators **500** einen differentiellen Zufallszahlengenerator **500** darstellt, d. h. einen Zufallszahlengenerator **500** unter Verwendung differentieller Signalverarbeitung in CMOS-Schaltungstechnik. Die CMOS-Schaltungstechnik ist besonders robust gegenüber externen Störungen.

[0116] Die Fläche des CMOS-Feldeffekttransistors **501**, der jeweils von dem Dekoder **506** ausgewählt wird, sollte erheblich kleiner sein, vorzugsweise um mindestens den Faktor 5, als die Fläche der weiteren CMOS-Feldeffekttransistoren **514**, **517**, **522**, **523**, **534**, **530**.

[0117] Weiterhin sollten der ausgewählte CMOS-Feldeffekttransistor **501** und der erste weitere CMOS Feldeffekttransistor **514** die gleiche Stromtreibfähigkeit aufweisen.

[0118] **Fig.** 6 zeigt einen Zufallszahlengenerator **600** für die parallele Erzeugung eines Zufallswortes gemäß einem weiteren Ausführungsbeispiel der Erfindung.

[0119] Der Zufallszahlengenerator **600** weist eine Vielzahl von CMOS-Feldeffekttransistoren **601** auf, die matrixförmig in einer Mehrzahl von Zeilen **602** und Spalten **603**

angeordnet sind.

[0120] Der Source-Anschluss **604** eines jeden CMOS-Feldeffekttransistors **601** ist mit jedem Source-Anschluss **604** eines jeden anderen CMOS-Feldeffekttransistors **601** gekoppelt sowie über eine Stromquelle **605** mit dem Massepotential **606**.

[0121] Der Gate-Anschluss **607** eines jeden CMOS-Feldeffekttransistors **601** ist mit jeweils einem Ausgang **608** eines Dekoders **609** gekoppelt, dessen Eingang **610** über eine Gate-Spannungsquelle **611** mit dem Massepotential **606** gekoppelt ist.

[0122] Die Drain-Anschlüsse **612** aller CMOS-Feldeffekttransistoren **601** sind miteinander sowie mit dem Massepotential **606** gekoppelt.

[0123] Die Source-Anschlüsse **604** von den sich jeweils in einer gleichen Zeile **602** befindenden CMOS-Feldeffekttransistoren **601** sind miteinander sowie mit jeweils einem Eingang **613** eines Multiplexers **614** gekoppelt.

[0124] Ein erster Ausgang **615** des Multiplexers **614** ist mit einem ersten Eingang **624** einer ersten Zufallszahlen-Umsetzungseinheit **616** gekoppelt, deren zweiter Eingang **615** an eine Speicher- und Steuerungseinheit **617** angeschlossen ist, mittels der sowohl die Gate-Spannung V_{Gate}, der Drain-Strom I_{Drain} der jeweiligen CMOS-Feldeffekttransistoren **601** und die im Zusammenhang mit dem Zufallszahlengenerator **500** aus **Fig.** 5 erläuterten Referenzspannung V_{ref} gesteuert werden.

[0125] Ein n-ter Ausgang **618** des Multiplexers **614** ist mit einem ersten Eingang **619** einer n-ten Zufallszahlen-Umsetzungseinheit **620** gekoppelt, deren zweiter Eingang **621** ebenfalls mit der Steuerungseinheit **617** gekoppelt ist.

[0126] An jedem Ausgang **625**, **626** der n Zufallszahlen-Umsetzungseinheiten **616**, **620** liegt jeweils ein Bit eines eine Zufallszahl repräsentierenden Ausgangssignalwerts an, welche gemeinsam, d. h. anschaulich im Parallelbetrieb, die Zufallszahl **622** erzeugen.

[0127] Der in **Fig.** 6 dargestellte Zufallszahlengenerator **600** eignet sich insbesondere zum Erzeugen einer längeren binären Zufallszahl, da das Erzeugen der Zufallszahl mittels des Zufallszahlengenerator **600** parallelisiert ist.

[0128] In diesem Zusammenhang ist es vorteilhaft, die CMOS-Feldeffekttransistoren **601** aus demselben Array, d. h. derselben Matrix für die verschiedenen Bits der Zufallszahl zu verwenden.

[0129] Aus statistischen Gründen sollte in diesem Fall jedoch die Anzahl der Transistoren in der Matrix erhöht werden, um zu gewährleisten, dass eine ausreichende Zahl von CMOS-Feldeffekttransistoren **601** die gewünschten Anforderungen an die Gleichverteilung der Auftrittwahrscheinlichkeit der Besetzungszustände erfüllt.

[0130] In diesem Dokument sind folgende Veröffentlichungen zitiert:

[1] EP 0 930 665 A2

[2] US 5,706,218

Patentansprüche

1. Zufallszahlengenerator
mit einem Halbleiterbauelement mit mindestens einer elektrisch aktiven Störstelle in der Struktur des Halbleiterbauelements,
mit einer Besetzungs-Erfassungseinheit, die mit dem Halbleiterbauelement gekoppelt ist und die derart eingerichtet ist, dass eine Besetzung oder eine Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt werden kann, und
mit einer Zufallszahlen-Umsetzungseinheit, die mit der Besetzungs-Erfassungseinheit gekoppelt ist und die derart eingerichtet ist, dass aus der ermittelten Besetzung oder der ermittelten Änderung der Besetzung in der elektrisch aktiven Störstelle eine Zufallszahl gebildet wird.

2. Zufallszahlengenerator nach Anspruch 1, bei dem die mindestens eine elektrisch aktive Störstelle in der Kristallstruktur des Halbleiterbauelements angeordnet ist.

3. Zufallszahlengenerator nach Anspruch 2, bei dem die mindestens eine elektrisch aktive Störstelle in einer Grenzfläche der Kristallstruktur des Halbleiterbauelements angeordnet ist.

4. Zufallszahlengenerator nach einem der Ansprüche 1 bis 3, bei dem das Halbleiterbauelement ein in MOS-Technologie hergestelltes Halbleiterbauelement ist.

5. Zufallszahlengenerator nach einem der Ansprüche 1 bis 4, bei dem das Halbleiterbauelement ein in CMOS-Technologie hergestelltes Halbleiterbauelement ist.

6. Zufallszahlengenerator nach einem der Ansprüche 1 bis 5, bei dem das Halbleiterbauelement ein Feldeffettransistor ist.

7. Zufallszahlengenerator nach Anspruch 6, bei dem der Feldeffettransistor derart dimensioniert ist, dass der Feldeffettransistor im statistischen Durchschnitt genau eine elektrisch aktive Störstelle aufweist.

8. Zufallszahlengenerator nach einem der Ansprüche 1 bis 7, bei der die Zufallszahlen-Umsetzungseinheit derart eingerichtet ist, dass jeweils in einem Abstand einer vorgegebenen Zeitdauer die Besetzung oder die Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt werden kann.

9. Zufallszahlengenerator nach einem der Ansprüche 1 bis 8, bei der die Zufallszahlen-Umsetzungseinheit derart eingerichtet ist, dass der Übergang von einem ersten Besetzungszustand der elektrisch aktiven Störstelle in einen zweiten Besetzungszustand der elektrisch aktiven Störstelle oder der Übergang von dem zweiten Besetzungszustand der elektrisch aktiven Störstelle in den ersten Besetzungszustand der elektrisch aktiven Störstelle ermittelt werden kann.

10. Zufallszahlengenerator nach Anspruch 8, bei der die Zufallszahlen-Umsetzungseinheit derart eingerichtet ist, dass die vorgegebene Zeitdauer um ein Mehrfaches länger ist als eine durchschnittliche Zeit einer Änderung der Besetzung in der elektrisch aktiven Störstelle.

11. Zufallszahlengenerator nach einem der Ansprüche 1 bis 10,
mit einer Mehrzahl von Halbleiterbauelementen mit jeweils im statistischen Durchschnitt mindestens einer elektrisch aktiven Störstelle in der Struktur des jeweiligen Halbleiterbauelements,
wobei die Besetzungs-Erfassungseinheit mit allen Halbleiterbauelementen gekoppelt ist, und
mit einer Halbleiterbauelement-Auswahleinheit zum Auswählen eines Halbleiterbauelements, bei dem die Besetzung oder die Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt wird.

12. Zufallszahlengenerator nach einem der Ansprüche 6 bis 11, mit einer Gate-Spannungs-Justiereinrichtung, mittels der die an dem Feldeffekttransistor anliegende Gate-Spannung eingestellt werden kann.

13. Zufallszahlengenerator nach den Ansprüchen 6 und 11,
mit einer Spannungsquelle, die mit der Halbleiterbauelement-Auswahleinheit derart gekoppelt ist, dass die Halbleiterbauelement-Auswahleinheit die von der Spannungsquelle bereitgestellte Spannung an den

Gate-Anschluss des ausgewählten Feldeffekttransistors der Mehrzahl der Feldeffekttransistoren anlegt, und

bei dem die Drain-Anschlüsse aller Feldeffekttransistoren mit der Besetzungs-Erfassungseinheit gekoppelt sind.

14. Zufallszahlengenerator nach Anspruch 13, bei dem die Besetzungs-Erfassungseinheit einen Bandpass-Filter aufweist,

dessen erster Eingang mit den Drain-Anschlüssen der Feldeffekttransistoren gekoppelt ist und

dessen zweiter Eingang mit den Source-Anschlüssen der Feldeffekttransistoren gekoppelt ist.

15. Zufallszahlengenerator nach Anspruch 14, bei dem die Besetzungs-Erfassungseinheit einen Differenzverstärker aufweist, der zwischen das Bandpass-Filter und die Zufallszahlen-Umsetzungseinheit geschaltet ist.

16. Zufallszahlengenerator nach einem der Ansprüche 1 bis 15, bei dem die Zufallszahlen-Umsetzungseinheit als Komparator ausgestaltet ist.

17. Verfahren zum Erzeugen einer Zufallszahl,

bei dem bei einem Halbleiterbauelement, welches mindestens eine elektrisch aktive Störstelle in seiner Struktur aufweist, eine Besetzung oder eine Änderung der Besetzung in der elektrisch aktiven Störstelle ermittelt wird, und

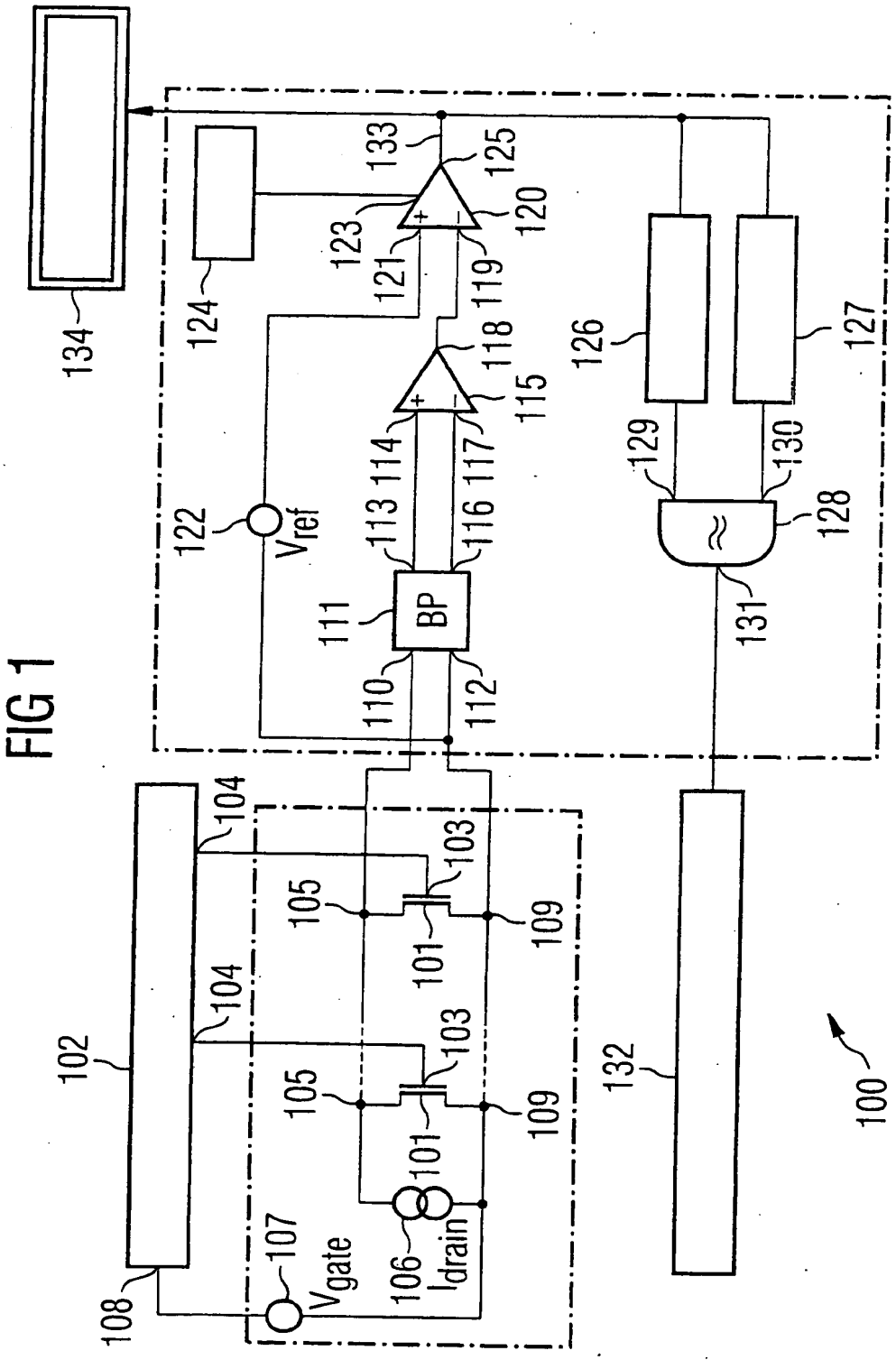
bei dem aus der ermittelten Besetzung oder der ermittelten Änderung der Besetzung in der elektrisch aktiven Störstelle eine Zufallszahl gebildet wird.

Hierzu 5 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 17 362 A1
Int. Cl.[7]: G 07 C 15/00
Offenlegungstag: 17. Oktober 2002

FIG 1



Nummer: DE 101 17 362 A1
Int. Cl.[7]: G 07 C 15/00
Offenlegungstag: 17. Oktober 2002

FIG 2B

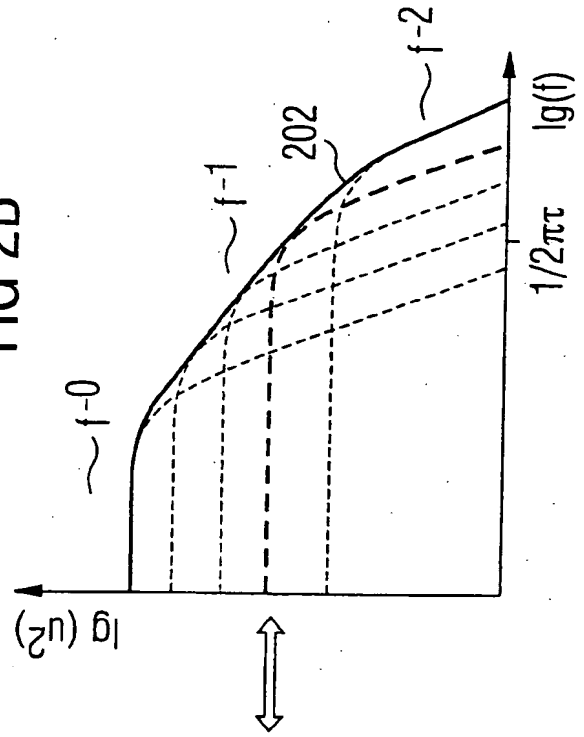
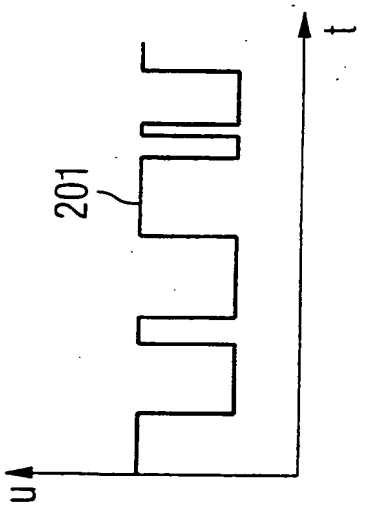


FIG 2A



Nummer: DE 101 17 362 A1
Int. Cl.[7]: G 07 C 15/00
Offenlegungstag: 17. Oktober 2002

FIG 3

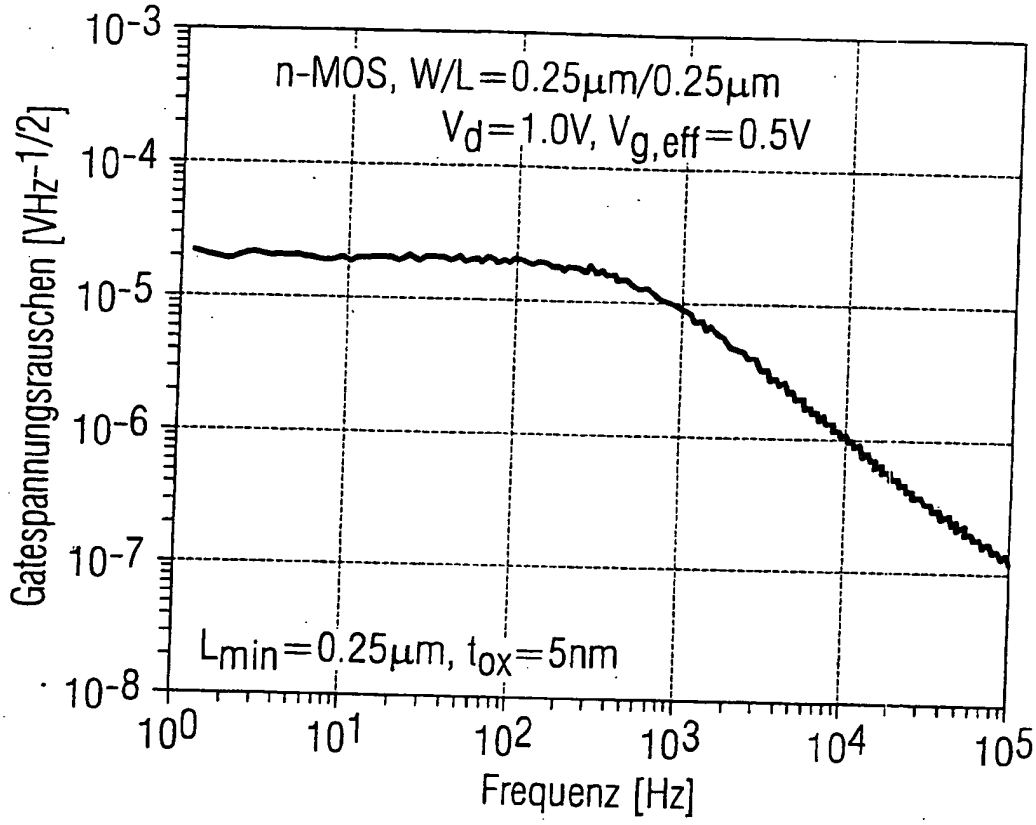
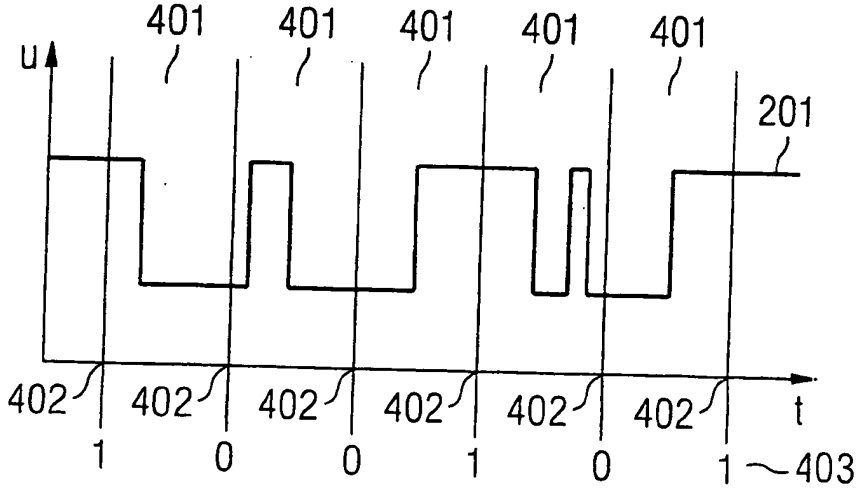
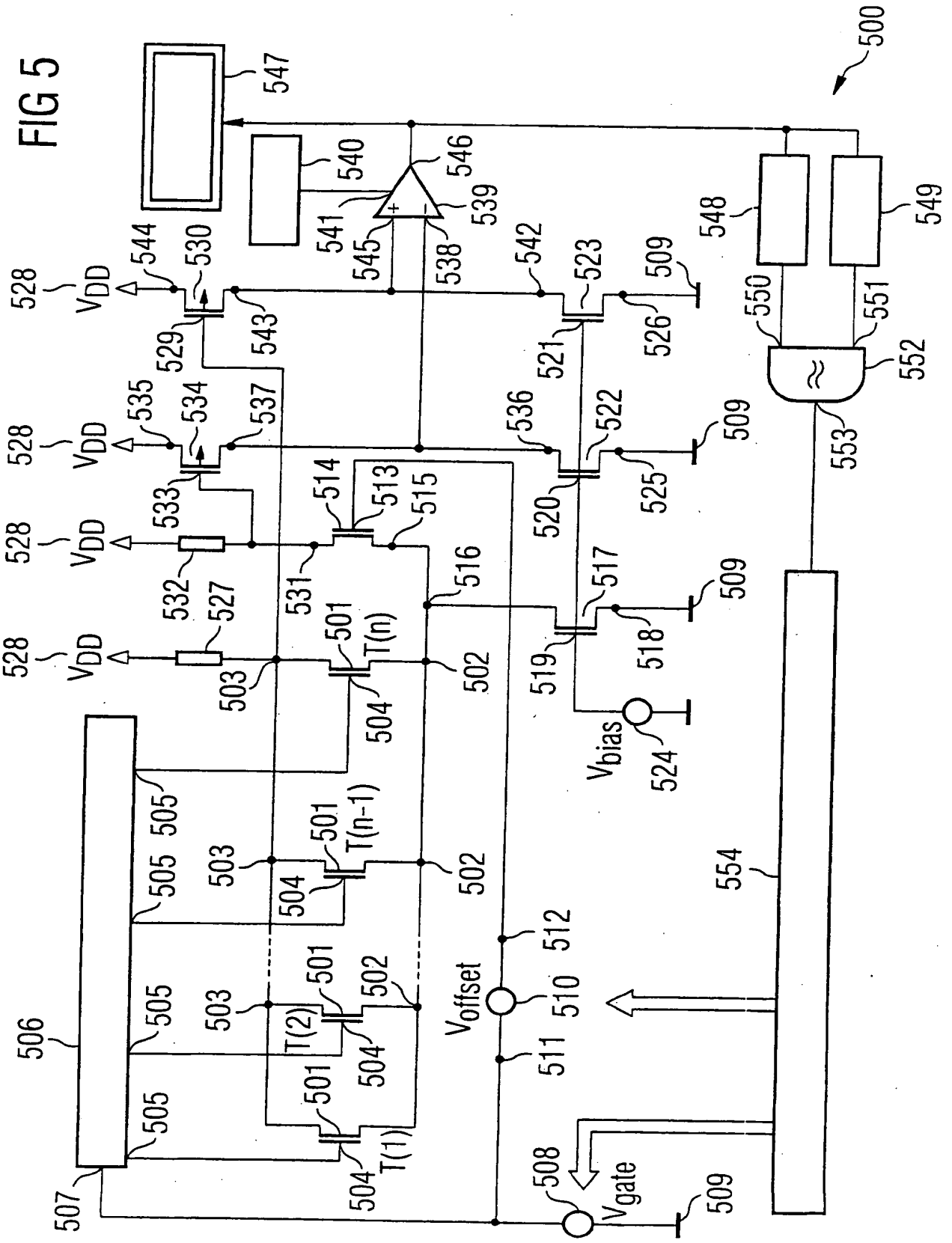


FIG 4



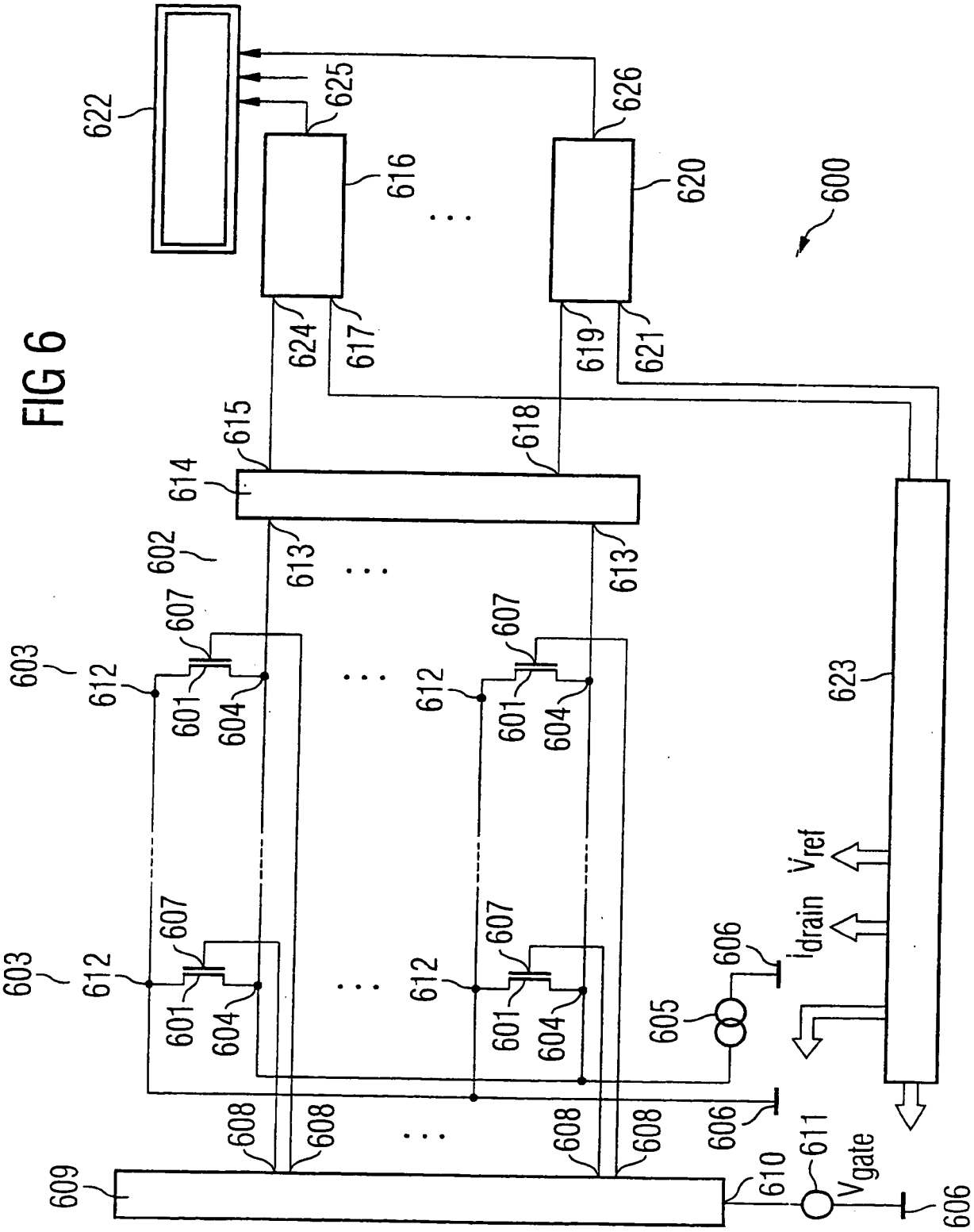
Nummer: DE 101 17 362 A1
Int. Cl.[7]: G 07 C 15/00
Offenlegungstag: 17. Oktober 2002

FIG 5



Nummer: DE 101 17 362 A1
Int. Cl.[7]: G 07 C 15/00
Offenlegungstag: 17. Oktober 2002

FIG 6



Zufallszahlengenerator und Verfahren zum Erzeugen einer Zufallszahl

Publication number:	DE10117362
Publication date:	2002-10-17
Inventor:	BREDERLOW RALF (DE)
Applicant:	INFINEON TECHNOLOGIES AG (DE)
Classification:	
- international:	***G06F7/58;*** **G06F7/58**; (IPC1-7): G07C15/00
- european:	G06F7/58R
Application number:	DE20011017362 20010406
Priority number(s):	DE20011017362 20010406

Also published as:

WO02082256 (A3
WO02082256 (A2
EP1379940 (A3)
EP1379940 (A2)
EP1379940 (A0)

more >>

Abstract of **DE10117362**

The invention relates to a random number generator comprising a number of semi-conductor elements comprising, on average, one electrically active disrupt cell in the frequency band which is important for processing, in the crystalline structure thereof. A suitable transistor is selected by a charge/detector unit and the charge thereof or an alteration of the charge in the electrically active disrupt cell of the selected transistor is determined. A random number is formed from the detected charge or alteration of the charg by means of a random number conversion unit.

This Page Blank (uspto)

Docket # 2004P00922

Applic. #

Applicant: Franke, et al.

Lerner Greenberg Stemer LLP
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101